JAN 04 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Koichi Shibata	Group Art Unit: 2131
Application No.: 09/726,423	Examiner: Taghi T Arani
Filed: December 1, 2000	Confirmation No.: 1425
For: PRINTING METHOD AND APPARATUS HAVING IMPROVED JOB SECURITY FUNCTION, AND COMPUTER PROGRAM PRODUCT EXECUTABLE BY COMPUTER FOR REALIZING IMPROVED JOB SECURITY FUNCTION	

REQUEST FOR RECONSIDERATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated October 25, 2004, Applicant respectfully requests reconsideration and withdrawal of the rejection of the claims.

All pending claims were rejected under 35 U.S.C. §103, on the grounds that they were considered to be "anticipated" by the Nezu patent (U.S. 5,638,511). For the reasons presented below, it is respectfully submitted that the Nezu patent neither anticipates, nor otherwise suggests, the claimed subject matter.

Claim 1 recites an apparatus for printing an image, that includes a receiving unit receiving print job data and a password corresponding to the print job data. As described in the specification, when the user sends a print job to the printer, the user also sends a password along with the print job, so that both are received by the printer. In rejecting claim 1, the Office Action indicates that the output means 2 of the Nezu patent corresponds

to the claimed receiving unit. However, this output means of the reference does not receive both print job data *and* a password corresponding to the print job data, as recited in the claim. Rather, in the system of the Nezu patent, when the output means, e.g. a print server, receives a print job, it *generates* a collation key and outputs it to the client who sent the print job. See, for example, Figures 11a and 11b, at step H86, as well as the corresponding description at column 11, lines 59-62, and column 18, lines 1-3, 32-33 and 45-51. In the system of the Nezu patent, the collation key is transmitted from the print server to the client PC, and is written to a removable storage medium, such as a floppy disk, in step H83. In order to print the job, the user must carry the floppy disk to the print server and load it into a disk drive at the print server. See, for example, column 24, lines 61-67.

Claim 1 goes on to recite a storage device that stores the print job data and the received password in correspondence with each other, a password taking unit, and a controller that permits the print job data to be printed when the password taken by the password taking unit matches the password stored in the storage device. The claim further recites that, when the password taken by the password taking unit is a prescribed password different from the password stored in the storage device, the controller permits a prescribed operation on the print job data stored in the storage device.

In connection with this last recitation, the Office Action refers to the Nezu patent at column 5, lines 31-37, which describes the use of a master code to unlock a locked stacker. This portion of the patent pertains to the second embodiment disclosed in connection with Figures 22-33 of the Nezu patent. As described in the patent, beginning at column 32, line 57, the first disclosed embodiment (discussed above) requires the user to go to the network

printer and load the portable storage medium in the printer, to start the printing operation. As a result, the user must wait at the printer until the job is completely printed, which could present an inconvenience for large print jobs. The second embodiment utilizes a different approach, wherein physical access to a printed job is restricted. In the second embodiment, the user is not required to present the collation key at the printer in order to initiate the print operation. Rather, printing begins as soon as a stacker, e.g. storage bin, is available in which to load the printed job. To maintain security of the printed job, the stacker is locked, so that no one other than the user can gain access to the printed materials.

The Nezu patent discloses that the lockable stackers can be dynamically allocated among different users. A problem could arise, therefore, if the users forgot to pick up their print jobs for a while, and the stackers remained locked for a long period of time. In such a case, new users would not be able to have secure jobs printed. To prevent this situation, at column 42, lines 5-12, the Nezu patent discloses that a manager may be provided with a master key to unlock stackers that have been closed for more than a predetermined period of time.

It is respectfully submitted that this disclosure has nothing to do with the subject matter recited in claim 1. In particular, the master key described in the Nezu patent relates to the ability of a manager to obtain access to print jobs that have already been completed and are stored in a facility that restricts physical access to the completed jobs. In contrast, claim 1 recites that, when a prescribed password is taken by the password taking unit, the controller permits a prescribed operation to be performed "on the print job data stored in said storage device." The master key disclosed in the Nezu patent does not have any effect upon print job data that is stored on the storage device, e.g. the hard disk 43, of the print

server. Nor does it relate to performing any type of prescribed operation on print job data, such as deletion or output to the printer. Rather, its only purpose is to permit the manager to gain access to a print job that has already been completed. By that time, the print data no longer exists on the hard disk.

Furthermore, it is respectfully submitted that the Nezu patent teaches away from the subject matter recited in the claims. As described in the present application, one of the problems that can arise with password-protected print jobs is that users may forget to complete the print job, as a result of which print job data can accumulate in the storage medium of the printer over time. In accordance with the claimed invention, a super user can present a prescribed password to enter into a mode of operation in which this accumulated print job data can be deleted or sent to the printer, to thereby remove it from the printer's storage medium.

The Nezu patent discloses a different approach to this type of problem. When a print job has a security designation, it is accompanied by information relating to a retention period, along with a designated method for processing the print job at the end of the retention period. See, for example, column 14, lines 42-45 and column 15, lines 8-11. When this retention period is exceeded, the print server cancels the holding of the print job, and processes the job according to the designated processing method. Thus, the Nezu patent discloses a technique for automatically removing the print job from the memory of the print server, after a designated period of time. In such a case, there is no need to employ a prescribed password to initiate a super user mode in which a prescribed operation, such as deletion or printing, is performed on print job data stored in the storage device.

For at least the foregoing reasons, it is respectfully submitted that the subject matter of claim 1 is neither anticipated, nor otherwise suggested, by the Nezu patent. For the same reasons, the subject matter of claims 8 and 15 is likewise patentable over the disclosure of this reference.

Other distinguishing features of the invention are recited in the various dependent claims. In light of the fundamental differences described above, however, it is believed that a detailed discussion of these other distinctions is unnecessary at this time.

Reconsideration and withdrawal of the rejection, and allowance of all pending claims is respectfully requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: January 4, 2005

By: _____
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620